IN THE CLAIMS:

Please amend the claims as follows.

1. (Currently amended) Apparatus for empirically adjusting a user's authorized access to a database, said apparatus comprising:

coupled to the database, a database discovery module configured to determine database structure and the user's authorized access ~~accesses~~ to the database, the user's authorized access including a set of authorized database tables and authorized columns;

coupled to the database, a command monitoring module configured to monitor the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns; and

coupled to the database discovery module and to the command monitoring module, an analysis module configured to compare the user's actual accesses with the user's authorized access ~~accesses~~ and configured to adjust the user's authorized access ~~accesses~~ taking into account results of the comparing by changing settings within a database access control module to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns. ~~operations by certain users on database tables and columns that were previously authorized but not observed by the command monitoring module.~~

2. (Previously presented) Apparatus of claim 1 further comprising, coupled to the database discovery module and to the analysis module, a storage area configured to accumulate data generated by the command monitoring module.

3. (Original) Apparatus of claim 1 wherein the command monitoring module is a sniffer.

4. (Original) Apparatus of claim 1 wherein the database is a relational database accessed by a structured query language.

5. (Currently amended) A computer-implemented method for empirically adjusting a user's authorized access to a database, said method comprising the steps of:

discovering the user's authorized access ~~accesses~~ to the database, the user's authorized access including a set of authorized database tables and authorized columns;

observing the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns;

comparing the user's actual accesses with the user's authorized access ~~accesses~~; and

adjusting the user's authorized database access ~~accesses~~ taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns. ~~operations by certain users on database tables and columns that were previously authorized but were not observed during the observing step.~~

6. (Currently amended) The method of claim 5 further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database.

7. (Canceled)

8. (Currently amended) The method of claim 5 wherein the discovering step uncovers any:

tables of the database;

columns of the database;

~~authorized users of the database;~~

views of the database;

stored procedures of the database;

user-defined functions of the database; and

triggers of the database.

9. (Currently amended) The method of claim 5 wherein the adjusting step further comprises at least one of:

suggesting revised database access control settings to a database administrator;

automatically hardening the database for all times of day;

automatically hardening the database selectively based on time of day;

alerting a database administrator; and

continuing to monitor the user's accesses to the database after conclusion of the observing step.

10. (Original) The method of claim 9 wherein the database is automatically hardened using standard SQL commands.

11. (Original) The method of claim 9 wherein the database is automatically hardened using database specific application programming interfaces.

12. (Canceled)

13. (Canceled)

14. (Currently amended) A computer-readable medium containing computer program instructions configured to empirically adjust a user's authorized access to a database, said computer program instructions performing the steps of:

discovering the user's authorized access ~~accesses~~ to the database, the user's authorized access including a set of authorized database tables and authorized columns;

observing the user's actual accesses to the database until a preselected quantity of actual accesses have been observed, the user's actual accesses including a set of accessed database tables and accessed columns;

comparing the user's actual accesses with the user's authorized access ~~accesses~~; and

adjusting the user's authorized database access ~~accesses~~ taking into account results of the comparing step by changing settings within a database access control module of a computer-implemented database server to deny the user future database access to an authorized database table or an authorized column that is not in the set of accessed database tables and accessed columns. ~~operations by certain users on database tables and columns that were previously authorized but were not observed during the observing step.~~

15. (Currently amended) The computer-readable medium of claim 14 further comprising the step of generating and storing at least one report based upon observing the user's actual accesses to the database.

16. (Canceled)

17. (Currently amended) The computer-readable medium of claim 14 wherein the discovering step uncovers any:

tables of the database;

columns of the database;

~~authorized users of the database;~~

views of the database;

stored procedures of the database;

user-defined functions of the database; and

triggers of the database.

18. (Currently amended) The computer-readable medium of claim 14 wherein the adjusting step further comprises at least one of:

suggesting revised database access control settings to a database administrator;

automatically hardening the database for all times of day;

automatically hardening the database selectively based on time of day;

alerting a database administrator; and

continuing to monitor the user's accesses to the database after conclusion of the observing step.

19. (Original) The computer-readable medium of claim 18 wherein the database is automatically hardened using standard SQL commands.

20. (Original) The computer-readable medium of claim 18 wherein the database is automatically hardened using database specific application programming interfaces.

21. (Canceled)

22. (Canceled)

23. (Previously presented) Apparatus of claim 1, wherein the preselected quantity of actual accesses is sufficiently large that all expected functionalities of applications accessing the database are exercised.

24. (Currently amended) The method of claim 5, further comprising:

storing data generated by the observing of the user's actual accesses to the database in a storage area.

25. (Previously presented) The method of claim 5, further comprising:

generating a map of which tables and columns of the database were accessed during the observing.

26. (Currently amended) The method of claim 5, further comprising:

monitoring the user's actual accesses to the database during an extended period occurring after the preselected quantity of actual accesses have been observed; and

generating an alert in real time regarding the user's actual accesses that are observed during the extended period that were not observed within the preselected quantity of the user's actual accesses.